

Minnesota Must Take the Lead to Protect Social Security Information, Private Data

By State Rep. Jim Davnie
Guest Columnist

Recent news accounts that Social Security numbers of up to 150,000 people who received grants from the U.S. Department of Agriculture were posted on a government website brought new urgency to discussions surrounding data privacy and consumer protection. While the Agriculture Department has removed the data and offered free credit monitoring to those individuals affected by the breach, it raises the question about who must be ultimately responsible for protecting sensitive personal information.

Originally, a Social Security number was a way for the government to track your earnings and pay retirement benefits. But over the years, it has become much more than that. It is the key to a lot of personal information and is commonly used as a form of identification by both private businesses and government agencies. In addition to legitimate uses like tax returns, student loan applications, mortgage transactions and mutual fund purchases, Social Security numbers were often used for things like student IDs, health insurance forms and insurance cards.

While these uses are being phased out gradually, there is also an emerging hidden market in which companies use Social Security numbers and other personal data as a commodity to be bought and sold. This widespread use of Social Security numbers in both the public and private sectors, combined with their key role in identity theft, has raised important worries about the ability of identity

thieves to gain access to them.

As concerns about identity theft have grown, opinions about data security have evolved. Early in the decade, consumers were advised to shred personal documents and remove Social Security numbers from their checks. Clearly, however, this approach left the burden of responsibility to the consumer. As Internet crime and identity theft has increased, people purchase costly software to protect personal data, again an approach that puts the bulk of the burden on individuals.

Once an individual has turned their Social Security number over to a private or government entity, it should be incumbent upon that entity to protect it. Minnesota has been on the leading edge of recognizing that responsibility. Bipartisan legislation over the past few years has been enacted to protect Social Security numbers and other private data such as credit card numbers. In 2005, we required private companies and the state to notify consumers if their private data had been breached. In 2006, we established the gold standard of identity theft protections by enacting a law that allows consumers to place a freeze on their credit reports for free if they are victims of identity theft, and for a minimal fee if they are not. We also prohibited the sale, lease or loan of Social Security numbers by businesses; however businesses that had already been selling, leasing or lending those numbers were allowed to continue. This

Guest column

Please see Page 4

Legislative Update

As of May 15, 2007, the Omnibus Data Practices bill (Senate File 596/House File 1360) has passed unanimously in both the Minnesota House and Senate. A conference committee has been named with the following members: (House) Simon, Holberg, Hillstrom, Hortman and Kahn; (Senate) Olson, Moua, Betzold, Limmer and Metzen.

As in past years, the bill contains a variety of technical and substantive changes, some of which impact only specific government entities and others that impact all entities subject to the Data Practices Act.

To find the current status or version of the bill online, go to www.leg.state.mn.us/leg/legis.asp and enter sf596 in the *bill number* box for Senate bills. Among the issues the bill addresses:

- Classification of data at the departments of Transportation and Revenue, and the Metropolitan Council;
- Extending the traveling data provision to the Judicial Branch;
- Data subject access to CriMNet's integrated search services;
- Technical change to substitute the longer phrase, "state agency, political subdivision and statewide system" for the shorthand-defined term of "government entity;"
- Social Security number changes;
- Access to drivers license photos by public defenders and criminal justice agencies; and
- Increased penalties for violation of the Data Practices Act.

From the IPAD Toolbox

Certain federal laws require that Minnesota government entities collect an individual's Social Security number (SSN). But according to the Federal Privacy Act of 1974 (5 U.S.C. 552a note - Disclosure of Social Security Number), if there is no federal law requiring the collection of an individual's SSN, and an entity asks for the SSN, the entity may not deny the individual any right, benefit or privilege if the individual refuses to provide his or her SSN. *Thus, the only time an individual must provide his/her SSN to a Minnesota government entity is when federal law requires it.*

Some federal laws that require the collection of an individual's SSN include:

- The Tax Reform Act of 1976 (42 U.S.C. 2025(e)(1)) – Authorizes the collection of SSNs for tax, public assistance, driver's license, or motor vehicle functions;
- The Family Support Act of 1988 (42 U.S.C. 3543(a)) – Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good cause for not requiring the number;
- The Higher Education Act Amendments of 1996 (31 U.S.C. 7701(c)) – Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms; and
- The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (42 U.S.C. 666(a)(13)) –

The following websites provide links to helpful information discussing issues surrounding the collection and use of Social Security numbers:

Social Security Administration

Identity Theft and Your Social Security Number
www.ssa.gov/pubs/10064.html

Federal Trade Commission

Identity Theft and Social Security Numbers
www.ftc.gov/os/testimony/040928test.shtm

Privacy Rights Clearinghouse

Social Security Numbers:
Frequently Asked Questions
www.privacyrights.org/fs/fs10a-ssnfaq.htm

My Social Security Number: How Secure Is It?
www.privacyrights.org/fs/fs10-ssn.htm

Electronic Privacy Information Center (EPIC)

Social Security Number Privacy Page
www.epic.org/privacy/ssn

Mandates that states have laws in effect that require collection of SSNs on various license applications, divorce and child support documents and death certificates.

IPAD Toolbox

Please see Page 4

Advice from the Swamp Fox*

*Francis Marion, "the Swamp Fox," was a colonial officer from South Carolina in the Revolutionary War renowned for hiding in swamps while carrying out guerilla warfare against the British.

can be found at www.ipad.state.mn.us/docs/ssnentity.pdf and www.ipad.state.mn.us/docs/ssnindividual.pdf.

The Swamp Fox

Dear Swamp Fox:

I am the Responsible Authority for the City of Spring Falls. Among other information, we collect the Social Security numbers (SSN) from our City employees for verification of employment eligibility. All employees must provide their SSNs on Form I-9, the Federal Employment Verification form. The City maintains these forms. I know that our employees must be given a Tennesen warning notice when SSNs are collected because it is a collection of private data from the employee about the employee. I am also aware of the requirements in the Federal Privacy Act notice when government entities collect SSNs. Could you provide a sample notice that includes the information the City should give to employees when we collect their SSNs for this employment purpose?

Interested Responsible Authority

Dear Interested Responsible Authority:

Thank you for submitting this question and I am encouraged that you are aware of the state and federal requirements placed on government entities when collecting SSNs. I would be happy to assist in providing language for a sample notice that slightly modifies the notice required by the Federal Privacy Act of 1974 (5 U.S.C. 552a note – Disclosure of Social Security Number) on Form I-9 to incorporate the state law requirements of the Tennesen warning notice. (Minnesota Statutes, section 13.04, subdivision 2.)

With the rising crime of identity theft, government entities must be especially careful in collecting SSNs and should only be collecting the numbers when they have specific legal authority. Clearly, the City has authority to collect employee SSNs on Form I-9 because the collection is mandated by federal law, specifically the Immigration Reform and Control Act of 1986 (8 U.S.C. 1324a).

I have created a sample notice that combines the federal and state requirements into five statements. Each statement is bolded and indicates whether it is based on federal or state law. Additional information about the state and federal notice requirements, including the specific language of the requirements,

Sample Notice

- **The authority to collect your Social Security number (SSN) is the Immigration Reform and Control Act of 1986, 8 U.S.C. 1324a.** [federal requirement]
- **Collection of your SSN is used to verify your employment eligibility and preclude unlawful employment of aliens not authorized to work in the United States.** [federal and state requirement]

[NOTE: Because IPAD is not in a position to know all permissible uses of SSNs by the City, the City must include the additional uses - if any - to complete this requirement.]

- **A known consequence for refusing to supply your SSN on this form is that you cannot begin employment with the City. A known consequence of supplying your SSN on this form is that the government entities listed below may have access to your SSN.** [state requirement]
- **Your SSN will be maintained by the City as a record of the basis used to determine your eligibility to work in the United States. The information will be kept by the City and may be made available to officials of the U.S. Immigration and Customs Enforcement, U.S. Department of Labor, and Office of Special Counsel for Immigration Related Unfair Employment Practices.** [state requirement]

[NOTE: Because IPAD is not in a position to know all persons and entities that may be authorized to access SSNs when collected by the City, the City must make that determination and include those additional persons or entities - if any - to complete this requirement.]

- **To be employed by the City, you are legally required to provide your SSN on this form.** [federal and state requirement]

IPAD Toolbox

Continued from Page 2

If an entity does not have federal authority to require an individual to provide his/her SSN, but wants to collect the SSN, the entity must consider the language in Minnesota Statutes, section 13.05, subdivision 3, that limits collection to situations that are necessary for the administration and management of programs authorized by state and federal law or local ordinance.

In addition, federal and state laws require that entities provide a specific notice when collecting an individual's SSN. (These notice requirements do not apply if an entity collects an adult individual's SSN from another adult individual.) IPAD has prepared two

new information pieces about the collection of SSNs. They are available on IPAD's website, www.ipad.state.mn.us/other_infomat.html.

Finally, as the crime of identity theft continues to grow, some organizations – public and private – are voluntarily eliminating their reliance on the SSN as an identifier. And, it is important to note, in 2005, the Minnesota Legislature enacted language that generally prohibits private entities, the University of Minnesota, and Minnesota State Colleges and Universities from assigning or using an individual's SSN as an identifier or part of an identifier. (Minnesota Statutes, section 325E.59.)

The Carpenter

Opinion Highlights

The following are highlights of recent advisory opinions by the Commissioner of Administration. All Opinions are available on the IPAD website, www.ipad.state.mn.us.

07-009: An individual asked whether School District 720, Shakopee, violated the data practices rights of a student relating to the district's collection of certain information. The Commissioner opined that because the district seemingly collected private data about the student from the student, the district should have provided the student with a Tennessee warning notice. (See Minnesota Statutes, section 13.04, subdivision 2.) In addition, the Commissioner

opined that because the district did not provide the required notice, the district could not use the data it collected.

07-010: The Inter Faculty Organization (IFO) asked whether Minnesota State University Moorhead (MSUM), which is a part of the Minnesota State Colleges and Universities System (MnSCU), properly denied access to a request for contingency plans MSUM may have for strikes by any groups of employees at MSUM. MSUM denied access to the data based on Minnesota Statutes, section 13.37, subdivision 1(a) – security information, and subdivision 1(c) – labor relations information. The Commissioner opined it is possible that some of the strike plan data are security information but that the data do not appear to fall under the definition of labor relations information.



**Information Policy
Analysis Division**

Questions or comments?

Contact the Information Policy Analysis Division at 201 Administration Building, 50 Sherburne Avenue, St. Paul, MN, 55155; phone 800.657.3721 or 651.296.6733; fax 651.205.4219; email info.ipad@state.mn.us.

Staff: Laurie Beyer-Kropuenske, *Director*, Stacie Christensen, Katie Engler, Janet Hey, Linda Miller, Leanne Phinney, and Catherine Scott.

This document can be made available in alternative formats, such as large print, Braille or audiotape by calling 651.296.6733.

For TTY communication, contact the Minnesota Relay Service at 800.627.3529 and ask them to place a call to 651.296.6733.

Copyright 2007 by the State of Minnesota, Department of Administration, Information Policy Analysis Division. All rights reserved.

Guest column

Continued from Page 2

year, legislation has been introduced to close that loophole while balancing the real need to use the data in necessary transactions.

A recent congressional report found that federal workers at 19 different agencies have lost personal information, potentially affecting thousands of employees and the public. Similar incidents have occurred in state agencies as well. Beyond tightening practices regarding the use of sensitive data, Minnesota can take the lead again to ensure private and public entities are responsibly protecting our information at the highest possible level.

Jim Davnie is the State Representative for Minnesota House District 62A and Chair of the House Labor and Consumer Protection Division.